UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
MIAMI DIVISION

EVEILYN PIERRE-LOUIS, and GUILLEN PIERRE-LOUIS, individually and on behalf of all others similarly situated, Plaintiffs, v. RETAIL DATA, LLC, Defendant.	Case No. _____ **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Eveilyn Pierre-Louis and Guillen Pierre-Louis ("Plaintiffs"), bring this Class Action Complaint against Defendant, Retail Data, LLC ("Defendant" or "Retail Data"), in their individual capacity and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiffs brings this class action complaint against Defendant for its failure to properly secure and safeguard the personally identifiable information ("PII") of Plaintiffs and other similarly situated current and former employees of Defendant ("Class Members"), including their names and Social Security numbers, likely among other information ("Private Information"). *See* Plaintiffs' Notification Letters, attached hereto as ***Exhibit A***.

2. On June 22, 2024, Defendant learned that cybercriminals had infiltrated its information systems and gained access to its files containing the PII of Plaintiffs and members of the proposed Class, including their names and Social Security numbers ("Data Breach").

3. On information and belief, the Data Breach included the theft of one terabyte of data, an extraordinary amount well beyond that of most data breaches.[1]

4. The Data Breach was perpetrated by RansomHub, a notorious cybergang operating out of Russia.[2]

5. Though Defendant says it responded immediately and hired a forensics team to investigate the Data Breach, Defendant's investigation took nearly seven weeks to determine that Plaintiffs' and Class Members' PII was affected.

6. Even after that lengthy seven-week investigation, Defendant still did not notify Plaintiffs until September 6, 2024, nearly a month after it admits it discovered that Plaintiffs were affected by Defendant's failures. Ex. A.

7. Defendant's unreasonable and unexplained delays prevented Plaintiffs from being able to timely protect themselves from the significantly increased risk of harm they must now face for years because of Defendant's disclosure of their Social Security numbers.

8. Defendant moreover expects Plaintiffs to take additional steps to protect themselves "from potential misuse of your information," including signing up for credit monitoring services, placing a security freeze on their accounts, reviewing financial account statements, and reviewing their credit reports. Ex. A.

9. Defendant received Plaintiffs and Class Members' Private Information in its provision of services to its clients for the benefit of Plaintiffs and Class Members.

---

[1] Halycon, *RansomHub Ransomware Hits Retail Data: 1 TB Exfiltrated* (Aug. 2, 2024), https://ransomwareattacks.halcyon.ai/attacks/ransomhub-ransomware-hits-retaildata-1tb-data-exfiltrated.

[2] *Id.*; Cybersecurity and Infrastructure Security Agency, *CISA and Partners Release Advisory on RansomHub Ransomware* (Aug. 29, 2024), https://www.cisa.gov/news-events/alerts/2024/08/29/cisa-and-partners-release-advisory-ransomhub-ransomware; *DarkWeb Profile: RansomHub*, https://socradar.io/dark-web-profile-ransomhub.

10. Plaintiffs brings this action on behalf of all persons whose PII was compromised because of Defendant's failure to: (i) adequately protect the PII of Plaintiffs and Class Members; (ii) timely warn Plaintiffs and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure its network containing such PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal statutes.

11. Although Defendant has not disclosed any information regarding how the Data Breach occurred or what it is doing to prevent another such incident in the future, Defendant's failures to implement reasonable, industry standard cybersecurity measures can be inferred by its failure to disclose any information concerning when the hackers first targeted Defendant, when they first infiltrated Defendant's information systems, how long they had such access, and whether Defendant knows for certain that the hackers have been fully and finally evicted from Defendant's information systems.

12. Indeed, if Defendant had the appropriate logging, monitoring, and alerting systems in place to timely identify malicious activity and alert Defendant of the same, then the above-outlined information would be known to Defendant and likely would have been known in time to prevent the hackers from exfiltrating Plaintiffs' and Class Members' PII.

13. Moreover, Defendant significantly delayed investigation and notification of the Data Breach strongly implied that Defendant lacked a serious and tested cybersecurity incident response plan, which is a core aspect of any reasonable, industry standard cybersecurity program.

14. By failing to implement these and other cybersecurity safeguards, Defendant blatantly disregarded the rights of Plaintiffs and the Class Members, including their right to control how their private information, including their Social Security numbers, are disseminated.

Defendant's failures are even more egregious given that Plaintiffs and Class Members cannot reasonably changed their Social Security numbers, like they could a credit card number.

15. Although Defendant recognizes the risk of sophisticated attacks, Defendant also represents that it appropriate protects PII in its Privacy Policy: "We have implemented appropriate technical and organizational security measures designed to protect the security of any personal information we process."[3]

16. In addition to the above failures, Plaintiffs required discovery to better understand the additional cybersecurity measures that Defendant failed to implement, given that Defendant has failed to include any of this information in its notification letter.

17. Because Defendant still maintains Plaintiffs' and Class Members' PII on its information systems, they have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

18. Because of Defendant's failures, Plaintiffs and Class Members have suffered concrete injuries, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (vi) experiencing an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and substantially increased risk of identity theft and financial fraud.

PARTIES

19. Plaintiffs are residents and citizens of Miami, Florida, where they intend to remain.

20. Plaintiff Eveilyn Pierre-Louis was employed at Defendant's location in North Miami Beach, Florida.

[3] https://retaildatallc.com/privacy-policy.

21. Plaintiff Guillen Pierre-Louis was employed at Defendant's locations in Sunrise, Florida, and Miami, Florida.

22. Defendant is a Virginia limited liability company with its principal place of business at 4461 Cox Road, Suite 300, Glen Allen, Virginia.

23. Defendant does substantial business in Florida, where both Plaintiffs were employed at Defendant's Florida locations, as detailed above.

24. Defendant's Florida registered agent is Corporation Service Company, 1201 Hays Street, Tallahassee, Florida, 32301.

JURISDICTION AND VENUE

25. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, there are thousands of Class Members, many of whom reside outside the state of Tennessee and have different citizenship from Defendant. Thus, minimal diversity exists under 28 U.S.C. §1332(d)(2)(A).

26. This Court has personal jurisdiction over Defendant because it employed Plaintiffs in this district and operate facilities in this District, where Plaintiffs were employed.

27. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to this action occurred in this District, including Defendant's collection of Plaintiffs PII.

ADDITIONAL FACTUAL ALLEGATIONS

13. Defendant is a business intelligence company that is "committed to providing reliable, accurate, and up-to-date data that helps our clients make informed decisions."[4]

[4] https://retaildatallc.com/about-us.

14. Defendant "is a leading provider of observational intelligence and auditing solutions for businesses of all sizes and industries. The company has a team of experienced professionals who are experts in collecting and analyzing data."[5]

15. Notwithstanding its failure to be transparent in its notification letters, Defendant represents that it "promise[s] to never share information about our clients or the data they have us collect."[6]

16. Defendant purports to have thirty-five years of experience in data collection, collecting more than 500 billion data points per week.[7]

17. With this level of data collection and with its level of experience, Defendant must understand the risks associated with data breaches, making its failure to prepare for this Data Breach and its failure to implement reasonable cybersecurity standards even more egregious.

18. Plaintiffs provided their PII to Defendant as a condition of their employment with Defendant.

19. Because of Defendant's failure to implement reasonable, industry standard cybersecurity safeguards, Plaintiffs' PII, including their Social Security numbers are now in the hands of identity thieves who entire mission is to perpetrate identity theft, financial fraud, and extortion.

20. The information held by Defendant in its computer systems at the time of the Data Breach included the unencrypted Private Information of Plaintiffs and Class Members.

21. Upon information and belief, Defendant made promises and representations to Plaintiffs and Class Members that their Private Information would be kept safe and confidential,

[5] *Id.*
[6] *Id.*
[7] *Id.*

that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

22. Plaintiffs' and Class Members' PII was provided to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access, especially because Defendant operates in the data collection industry.

23. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiffs and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep consumer's Private Information safe and confidential.

28. Defendant had obligations created by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"), industry standards, and representations made to Plaintiffs and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

29. Moreover, Defendant's duty to implement reasonable cybersecurity safeguards arose under Fla. Stat. 501.171(2), which provides that Florida companies who collect such PII "shall take reasonable measures to protect and secure data in electronic form containing personal information."

30. Defendant derived a substantial economic benefit from collecting Plaintiffs' and Class Members' PII. Without the required submission of PII, Defendant would not have been able to accept Plaintiffs employment services.

31. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting Plaintiffs' and Class Members' PII from disclosure, as such protection requirements are black-letter law in Florida.

Defendant's Data Breach Was Imminently Foreseeable.

32. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting institutions that collect and store PII, like Defendant, preceding the date of the Data Breach.

33. Indeed, the Data Breach should have been even more foreseeable because Defendant operations in the data collection industry and thus should be among the most informed companies regarding the threats associated with the collection of sensitive information.

34. Data thieves regularly target institutions like Defendant due to the highly sensitive information in their custody. Defendant knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

35. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[8]

36. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the PII it collected and maintained would be targeted by cybercriminals.

37. As a custodian of PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiffs and Class Members, and of the foreseeable

[8] *See* Identity Theft Res. Ctr., *2021 Data Breach Annual Report*, at 6 (Jan. 2022), https://notified.idtheftcenter.org/s/.

consequences if its data security systems were breached, including the significant costs imposed on Plaintiffs and Class Members because of a breach.

38. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

39. Defendant was, or should have been, fully aware of the unique type and the significant volume of data in its systems, amounting to potentially thousands of individuals' detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

40. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

41. The ramifications of Defendant's failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

Value of Personally Identifiable Information

42. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[9] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer

[9] 17 C.F.R. § 248.201 (2013).

or taxpayer identification number."[10]

43. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[11]

44. For example, PII can be sold at a price ranging from $40 to $200.[12] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[13]

45. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a typical retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach—including Social Security number—is impossible to "close" and difficult, if not impossible, to change.

46. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[14]

47. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also

---

[10] *Id.*

[11] *Your personal data is for sale on the dark web. Here's how much it costs,* DIGITAL TRENDS, Oct. 16, 2019, https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

[12] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN, Dec. 6, 2017, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

[13] *In the Dark*, VPNOVERVIEW, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

[14] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[15]

Defendant Failed to Comply with FTC Guidelines and Florida Statutory Requirements.

48. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the FTCA, 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

49. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal consumer information they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

[15] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

50. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

51. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

52. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of its data security practices, or to appropriately prepare to face a data breach and respond to it in a timely manner. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

53. Defendant was at all times fully aware of its obligation to protect the PII of consumers under the FTCA yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

54. Defendant's failure is even more clear given the timeline and notification letters

they sent to Plaintiffs. Defendant apparently discovered the Data Breach on June 22, 2024, but Defendant took until August 9 to discover that Plaintiffs' information was included and then failed to send out notification letters for almost another month. These unreasonable delay in responding to the Data Breach strongly implies that Defendant lacked a reasonable cybersecurity incident response plan, as is required by industry standards and FTC expectations.

55. Moreover, Defendant failed to explain when the hackers gained access, how long they were in Defendant's information systems, or whether and how Defendant knows the hackers were evicted from Defendant's information systems. This strongly implies that Defendant failed to implement the required monitoring, logging, and alerting safeguards that are a part of all reasonable, industry standard cybersecurity programs and would have provided them with this information and alerting sufficient to stop the attack before data theft could occur. These systems include endpoint detection and response, extended detection and response, data loss prevention tools, and centralized logging and alerting systems.

56. Still further, because it operates in Florida and collects the PII of its Florida employees, Defendant had an obligation to under black-letter Florida law to implement the same reasonable, industry standard cybersecurity safeguards, pursuant to Fla. Stat. 501.171(2).

Defendant Failed to Comply with Industry Standards.

57. Experts studying cybersecurity routinely identify institutions that store PII like Defendant as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

58. Some industry best practices that should be implemented by institutions dealing with sensitive PII, like Defendant, include, but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware

software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

59. Other best cybersecurity practices that are standard at large institutions that store PII include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach and Defendants failure to understand how the Data Breach occured, Defendant failed to follow these cybersecurity best practices.

60. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

61. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

Common Injuries & Damages

62. Because of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (a)

invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their PII; (e) invasion of privacy; and (f) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII.

The Data Breach Increases Victims' Risk of Identity Theft.

63. Plaintiffs and Class Members are at a heightened risk of identity theft for years to come, especially because Defendant's failures resulted in Plaintiffs' and Class Members' Social Security number falling into the hands of identity thieves.

64. The unencrypted PII of Class Members has already or will end up for sale on the dark web because that is the *modus operandi* of hackers. Indeed, when these criminals do not post the data to the dark web, it is usually at least sold on private Telegram channels to even further identity thieves who purchase the PII for the express purpose of conducting financial fraud and identity theft operations.

65. Further, the standard operating procedure for cybercriminals is to use some data, like the Social Security numbers here, to access "fullz packages" of that person to gain access to the full suite of additional PII that those cybercriminals have access through other means. Using this technique, identity thieves piece together full pictures of victim's information to perpetrate even more types of attacks.[16]

[16] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning

66. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

67. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

Loss of Time to Mitigate Risk of Identity Theft and Fraud

68. Because of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm and a Defendant arguing that the individual failed to mitigate damages.

69. By spending this time, data breach plaintiffs are not manufacturing their own harm,

---

credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm.

they are taking necessary steps at Defendant's direction and because the Data Breach included their Social Security number.

70. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience because of the Data Breach, such as contacting credit bureaus to place freezes on their accounts; changing passwords and re-securing their own computer networks; and checking their financial accounts and health insurance statements for any indication of fraudulent activity, which may take years to detect.

71. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[17]

72. These efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[18]

[17] *See* United States Government Accountability Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/new.items/d07737.pdf.
[18] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps.

Diminution of Value of PII

73. PII and PHI are valuable property rights.[19] Their value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates beyond a doubt that PII has considerable market value.

74. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[20]

75. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[21,22]

76. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[23]

77. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."

78. Because of the Data Breach, Plaintiffs' and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by

---

[19] *See, e.g.*, Randall T. Soma, et al., Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).
[20] https://www.latimes.com/business/story/2019-11-05/column-data-brokers.
[21] https://datacoup.com.
[22] https://digi.me/what-is-digime/.
[23] Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

79. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, and of the foreseeable consequences that would occur if their data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

80. Defendant was, or should have been, fully aware of the unique type and the significant volume of data in its network, amounting to likely thousands of individuals' detailed personal information, upon information and belief, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

81. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

The Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary.

82. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes.

83. Such fraud may go undetected for years; consequently, Plaintiffs and Class

Members are at a present and continuous risk of fraud and identity theft for many years into the future.

84. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor and protect Class Members from the risk of identity theft that arose from the Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

Plaintiffs' Experience

85. Plaintiffs provided their PII to Defendant as a condition of their employment with Defendant in Florida.

86. At the time of the Data Breach, Defendant retained Plaintiffs' PII in its system.

87. Plaintiffs' PII was compromised in the Data Breach and stolen by identity thieves who illegally accessed Defendant's network for the specific purpose of targeting the PII.

88. Plaintiffs take reasonable measures to protect their PII.

89. Plaintiffs store any documents containing their PII in a safe and secure location and diligently chooses unique usernames and passwords for their online accounts.

90. Because of the Data Breach, Plaintiffs has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. They have and will continue to monitor accounts and credit scores and have sustained emotional distress. This is time that was lost and unproductive and took away from other activities and work duties.

91. Plaintiffs also suffered actual injury in the form of damages to and diminution in the value of their PII—a form of intangible property that he entrusted to Defendant for the purpose of obtaining services from Defendant, which was compromised in and because of the Data Breach.

92. Plaintiffs suffered lost time, interference, and inconvenience because of the Data Breach and has anxiety and increased concerns for the loss of their privacy.

93. Plaintiffs has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their PII, especially their name and Social Security number, being placed in the hands of criminals.

94. Defendant obtained and continues to maintain Plaintiffs' PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Plaintiffs' PII was compromised and disclosed because of the Data Breach.

95. As a result of the Data Breach, Plaintiffs anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiffs is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

CLASS ALLEGATIONS

96. Pursuant to Federal Rules of Civil Procedure 12(b)(2), 23(b)(3), and 23(c)(4), Plaintiffs brings this action on behalf of themselves and on behalf of all members of the proposed class defined as:

> All individuals residing in the United States whose PII was compromised in the Data Breach ("Class").

97. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

98. Plaintiffs reserves the right to amend the definition of the proposed Class or to add

a subclass before the Court determines whether certification is appropriate.

99. The proposed Class meets the criteria certification under Federal Rule of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3).

100. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, Plaintiffs believes the proposed Class includes thousands of individuals who have been damaged by Defendant's conduct as alleged herein. The precise number of Class Members is unknown to Plaintiffs but may be ascertained from Defendant's records.

101. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant's conduct violated the FTC Act and Fla. Stat. § 501.171(2);

c. When Defendant learned of the Data Breach;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII compromised in the Data Breach;

e. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

f. Whether Defendant's data security systems, prior to and during the Data Breach, were consistent with industry standards;

g. Whether Defendant owed duties to Class Members to safeguard their PII;

h. Whether Defendant breached their duties to Class Members to safeguard their PII;

i. Whether hackers obtained Class Members' PII via the Data Breach;

j. Whether Defendant had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

k. Whether Defendant breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

l. Whether Defendant knew or should have known its data security systems and monitoring processes were deficient;

m. What damages Plaintiffs and Class Members suffered as a result of Defendant's misconduct;

n. Whether Defendant's conduct was negligent;

o. Whether Defendant breached contracts it had with its clients, which were made expressly for the benefit of Plaintiffs and Class Members;

p. Whether Plaintiffs and Class Members are entitled to damages;

q. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

r. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

102. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII, like that of every other Class Member, was compromised in the Data Breach. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Defendant. Plaintiffs is advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class Members arise

from the same operative facts and are based on the same legal theories.

103. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

104. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members. For example, all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

105. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

106. Class certification is also appropriate under Federal Rule of Civil Procedure 23(b)(2). Defendant has acted and/or refused to act on grounds generally applicable to the Class

such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

107. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach, as is evident by Defendant's ability to send those individuals notification letters.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE AND NEGLIGENCE PER SE
(On Behalf of Plaintiffs and the Class)

108. Plaintiffs incorporates the above allegations as if fully set forth herein.

109. Plaintiffs and Class Members provided their non-public PII to Defendant in connection with and as a condition of their employment with Defendant's.

110. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed.

111. By assuming the responsibility to collect and store this data, Defendant had duties of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

112. Defendant had duties to employ reasonable security measures under Section 5 of the FTCA, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

113. Defendant's duty to use reasonable security measures also arose under Fla. Stat. § 501.171(2), which mandates that Defendant implement reasonable cybersecurity measures.

114. Defendant owed a duty of care to Plaintiffs and Class Members to provide data

security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the PII.

115. Moreover, Defendant had a duty to promptly and adequately notify Plaintiffs and Class Members of the Data Breach.

116. Defendant had and continues to have duties to adequately disclose that the PII of Plaintiffs and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice is necessary to allow Plaintiffs and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

117. Defendant breached its duties, pursuant to the FTCA, Fla. Stat. § 501.171(2), and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of its networks and systems, including by failing to implement reasonable monitoring, logging, and alerting systems such as EDR/XDR and a centralized security event management system;

c. Allowing unauthorized access to Class Members' PII;

d. Failing to detect in a timely manner that Class Members' PII had been compromised;

e. Failing to remove Plaintiffs' and Class Members' PII it was no longer required to retain pursuant to regulations; and

f. Failing to implement a reasonable cybersecurity incident response plan that would have enabled Defendant to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so they could take appropriate steps to mitigate the potential for identity theft and other damages.

118. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and Class Members.

119. Defendant's violation of the FTC Act and Fla. Stat. § 501.171 also constitutes negligence *per se*, as those provisions are designed to protect individuals like Plaintiffs and the proposed Class Members from the harms associated with data breaches.

120. Defendant has admitted that the PII of Plaintiffs and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

121. But for Defendant's wrongful and negligent breaches of duties owed to Plaintiffs and Class Members, the PII of Plaintiffs and Class Members would not have been compromised.

122. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiffs and Class Members and the harm, or risk of imminent harm, suffered by Plaintiffs and Class Members. The PII of Plaintiffs and Class Members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

123. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy;

(ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (xi) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

124. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

125. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PII in its continued possession.

126. Plaintiffs and Class Members are therefore entitled to damages, including restitution and unjust enrichment, declaratory and injunctive relief, and attorneys' fees, costs, and expenses.

127. Given Defendant's failures to implement the proper systems, as defined above, even knowing the ubiquity of the threat of data breaches, Defendant's decision not to invest enough

resources in its cyber defenses amounts to gross negligence.

COUNT II
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

128. Plaintiffs incorporates Paragraphs 1 through 107 above if fully set forth herein.

129. Plaintiffs brings this claim in the alternative to their breach of third-party beneficiary contract claim above.

130. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they provided Defendant with their PII. In exchange, Defendant should have provided adequate data security for Plaintiffs and Class Members.

131. Defendant knew that Plaintiffs and Class Members conferred a benefit on it in the form their PII as a necessary part of their receiving services from Defendant's clients. Defendant appreciated and accepted that benefit. Defendant profited from these transactions and used the PII of Plaintiffs and Class Members for business purposes.

132. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments on behalf of or for the benefit of Plaintiffs and Class Members.

133. As such, a portion of the payments made for the benefit of or on behalf of Plaintiffs and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

134. Defendant, however, failed to secure Plaintiffs and Class Members' PII and, therefore, did not provide adequate data security in return for the benefit Plaintiffs and Class Members provided.

135. Defendant would not be able to carry out an essential function of its regular

business without the PII of Plaintiffs and Class Members and derived revenue by using it for business purposes. Plaintiffs and Class Members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

136. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

137. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their PII, they would not have allowed their PII to be provided to Defendant.

138. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profit at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their PII.

139. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money wrongfully obtained from Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

140. Plaintiffs and Class Members have no adequate remedy at law.

141. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of

benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (xi) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

142. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

143. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

COUNT III
BREACH OF BAILMENT
(On Behalf of Plaintiffs and the Class)

144. Plaintiffs incorporate Paragraphs 1 through 107 above as if fully set forth herein.

145. Plaintiffs conveyed their PII to Defendant lawfully as a condition of employment with the understanding that Defendant would return or delete their PII when it was no longer required.

146. Defendant accepted this PII on the implied understanding that Defendant would honor its obligations under federal regulations, state law, and industry standards to safeguard Plaintiffs' PII and act on the PII only within the confines of the purposes for which Defendant collected Plaintiffs' PII.

147. By failing to implement reasonable cybersecurity safeguards, as detailed above, Defendant breached this bailment agreement causing harm to Plaintiffs in the form of violations of their right to privacy and to self-determination of who had/has access to their private information, in the form of requiring them to spend their own valuable time responding to Defendant's failures, and in the form of forcing Plaintiffs and the Class to face years of substantially increased risk of identity theft and financial fraud.

PRAYER FOR RELIEF

WHEREFORE**,** Plaintiffs, on behalf of themselves and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class, pursuant to Federal Rule of Civil Procedure 23;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all

applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures; requiring Defendant to segment data by, among other things, creating firewalls and access

controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

ix. requiring Defendant to conduct regular database scanning and securing checks;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendant to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats,

both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvi. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of actual damages, compensatory damages, and nominal damages, in an amount to be determined, and for punitive damages, as allowable by law;

E. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;

F. Pre- and post-judgment interest on any amounts awarded; and

G. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all issues so triable.

Dated: September 12, 2024

Respectfully submitted,

/s/ Jeff Ostrow
Jeff Ostrow FBN 121452
Steven Sukert FBN 1022912
KOPELOWITZ OSTROW P.A.
1 W. Las Olas Blvd., Ste. 500
Fort Lauderdale, FL 33301
Telephone: (954) 525-4100
ostrow@kolawyers.com
sukert@kolawyers.com

J. Gerard Stranch, IV (TN BPR # 23045)*
Grayson Wells (TN BPR # 039658)*
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel: (615) 254-8801
gstranch@stranchlaw.com
gwells@stranchlaw.com

**Application for admission* pro hac vice *forthcoming*

Counsel for Plaintiffs and the Putative Class